



Operating the Cisco ICS 7750

This chapter explains how to operate the Cisco Integrated Communications System 7750 (Cisco ICS 7750) after initial configuration is complete. The chapter is organized as follows:

- [Accessing the System, page 5-1](#)
- [Backing Up System Data, page 5-23](#)
- [Setting Security Privileges, page 5-30](#)
- [Setting Security Privileges, page 5-30](#)
- [Shutting Down the System, page 5-31](#)

Accessing the System

This section tells how to access the Cisco ICS 7750 and gives guidelines for best practices when accessing the system:

- [Accessing the System During Initial Configuration, page 5-2](#)
- [Accessing the System After Initial Configuration, page 5-2](#)
- [Accessing ICSCfg, page 5-4](#)
- [Accessing ICS System Manager, page 5-4](#)
- [Navigating in ICS System Manager, page 5-5](#)
- [Using ICS System Manager, page 5-6](#)
- [Accessing Cisco CallManager, page 5-8](#)

- [Accessing SPE310s, page 5-8](#)
- [Best Practices for Using Microsoft SQL Server, page 5-14](#)
- [Best Practices for Configuring DHCP, page 5-15](#)
- [Best Practices for Using the Cisco IOS CLI, page 5-16](#)
- [Using Peripherals with SPE310s, page 5-19](#)

Accessing the System During Initial Configuration

When configuring the system for the first time, you can use a web browser to perform most tasks. See [Chapter 4, “Completing the Cisco ICS 7750 Installation,”](#) for system installation and configuration instructions.

Accessing the System After Initial Configuration

After system installation and configuration, you have many ways to access the system:

- Cisco browser-based software interfaces:
 - ICSCfg—The Cisco ICS System Manager initial configuration program (ICSCfg) enables you to specify key system parameters during initial configuration and to change those parameters at any time after initial configuration. For additional information, see the [“Accessing ICSCfg” section on page 5-4](#).
 - ICS System Manager—ICS System Manager is preinstalled on the Cisco System Processing Engine 310 (SPE310) running System Manager, in chassis slot 6. You can use ICS System Manager to access, configure, monitor, and manage the chassis, its cards, and the interconnected Catalyst switches. For additional information, see the [“Accessing ICS System Manager” section on page 5-4](#).
 - Cisco CallManager—You can install Cisco CallManager on SPE310s and use the software to configure call admission control, route plans, voice gateways (typically multiservice route processors [MRPs] or analog station interfaces [ASIs]), Cisco IP Phones, and other features

associated with transmitting voice traffic over an IP network. For additional information, see the [“Accessing Cisco CallManager” section on page 5-8](#).

- Cisco IOS software command-line interface (CLI)—You can use Cisco IOS software to configure ASIs, MRPs, and SSPs. For additional information, see the [“Accessing the Cisco IOS CLI on ASIs, MRPs, and the SSP Through Telnet” section on page 5-11](#).

- Microsoft Windows software interfaces:

- Terminal Services Client—You can use Terminal Services Client to access the SPE310 desktop and perform standard Windows file management operations on the SPE310. For additional information, see the [“Accessing SPE310s” section on page 5-8](#).

Terminal Services Client is packaged with Windows 2000. Terminal Services Client is also available for downloading and installing on to other Windows operating systems. See the [“Installing Microsoft Terminal Services Client” section on page 2-19](#) for installation instructions.

- Terminal emulation interfaces—You can use native tools such as Telnet and HyperTerminal to configure system cards. You can also connect directly to the system alarm processor (SAP) through a console or modem connection and troubleshoot system cards. For additional information, see the [“Accessing Processor Cards Through the SAP” section on page 5-12](#).

- Simple Network Management Protocol (SNMP)–based Management Information Base (MIB)—You can use the SNMP MIB to manage the Cisco ICS 7750 with software such as CiscoWorks2000 and HP OpenView. (For additional information, see the [“Using Network Management Solutions with the Cisco ICS 7750” section on page 6-146](#).)

Accessing ICSConfig

Follow these steps to access ICSConfig.

**Note**

This section describes ICSConfig functionality after initial configuration is complete. For a description of ICSConfig functionality during initial configuration, see [Chapter 4, “Completing the Cisco ICS 7750 Installation.”](#)

-
- Step 1** On a PC, open Netscape Communicator or Microsoft Internet Explorer.
- Step 2** In the Location or Address field, enter the following URL, replacing *IP address* with the IP address of the SPE310 running System Manager:
- `http://IP address/icsconfig`**
- Step 3** Log in as an administrator (user ID *administrator*), and enter your password (the default is *changeme*).
- Step 4** Click **OK**.
- The system discovers the cards that are currently installed in the chassis. After the discovery process is complete, the ICS 7700 System Configuration page displays.
- Step 5** Click **ICS 7700 System Setup**.
- Step 6** Make any desired changes to the system parameters, and submit your changes.
- It will take up to 20 minutes for the system to process your changes. When the STATUS LEDs on the SPE310s change to solid green, the submit process is complete.
-

Accessing ICS System Manager

You can use ICS System Manager to access, configure, monitor, and manage the chassis and its cards.

When you have installed and configured your system as described in [Chapter 4, “Completing the Cisco ICS 7750 Installation,”](#) follow these steps to access ICS System Manager:

-
- Step 1** On a PC, open Netscape Communicator or Microsoft Internet Explorer.
- Step 2** In the Location or Address field, enter the following URL, replacing *IP address* with the IP address of the SPE310 running System Manager:

http://IP address/ics



Note If you do not know the IP address of the SPE310, see the [“Determining the IP Address of an SPE310”](#) section on page 5-22.

- Step 3** Log in as the super administrator (user ID is *admin*), and enter your password (the default is *admin*).
- Step 4** Click **Login**.
-

Navigating in ICS System Manager

To navigate in ICS System Manager, click the tabs that are visible at the top of every ICS System Manager page:

- **Home**—Displays a page in which you can toggle between a short summary (Summary View) and a detailed list (Detailed View) of information about system cards.
- **Configure**—Displays a page in which you can choose any of the following utilities:
 - **SSP Manager**—Enables you to configure the system switch processor (SSP) and to perform LAN management tasks, such as administering workgroup changes and using link statistics to troubleshoot problems.
 - **System Setup**—Enables you to view system parameters and provides instructions for changing the parameters.

- Fan Manager—Enables you to view and update information related to the planned replacement of the fan tray.
- COM Port Manager—Enables you to view and change system port assignments (other than the SAP console port).
- Applications—Provides one or more links to applications such as Cisco CallManager.
- Monitor—Displays a page that shows current data about your system, such as the number of bytes transferred over an Ethernet port or the amount of disk space used on an SPE310.
- Event Manager—Displays a page in which you can set preferences for logging and event notifications, define rules for the reporting of system events, set up event reports, and view system events.
- Software Upgrade—Displays a page from which you can upload and install Cisco IOS software images for ASIs, MRPs, and SSPs, and firmware for the SAP. For additional information, see the *Cisco ICS 7750 Release Notes* for the release to which you are upgrading.
- Security—Displays a page for assigning users to groups with different security levels.
- System Maintenance—Displays a page for scheduling and running backups of system software data and viewing instructions on restoring system software data.

Using ICS System Manager

This section tells how to use ICS System Manager to perform the following routine tasks:

- [Determining the ICS System Manager Version](#)
- [Determining the Cisco IOS Software Release Running on the SSP](#)



Note

For additional information about how to use ICS System Manager, refer to the ICS System Manager online help.

Determining the ICS System Manager Version

The ICS System Manager bundle version number is displayed on the System Manager home page, in a box just under the graphic representation of the system chassis.

For example:

Software Bundle:

V<version number>

Running since:

<date and time ICS System Manager was last restarted>

The ICS System Manager home page also lists the cards currently running in the system chassis, as well as their assigned IP addresses and the software running on each. You can switch between a summary view and a detailed view of the hardware and software installed on the cards in the system.

Determining the Cisco IOS Software Release Running on the SSP

You can use ICS System Manager to determine the Cisco IOS software release that is running on the SSP, as well as other information about the SSP, as follows:

-
- Step 1** Click the **Configure** tab on the ICS System Manager home page.
 - Step 2** Click **SSP Manager**.
 - Step 3** If prompted, log in as an administrator (user ID *administrator*), and enter your password (the default is *changeme*).
 - Step 4** Click **show tech-support**.

The system invokes the **show version** command on the SSP. The following is sample output from this command:

```
Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5.2)XU,
MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2000 by Cisco Systems, Inc.
```

Additional output lines from the **show version** command include information such as the processor revision numbers and the amount of available memory.

Accessing Cisco CallManager

You can install Cisco CallManager on SPE310s and use the software to configure call admission control, route plans, voice gateways (such as MRPs or ASIs with installed voice interface cards [VICs] or voice WAN interface cards [VWICs]), Cisco IP Phones, and other features associated with transmitting voice traffic over an IP network.

To access Cisco CallManager on the Cisco ICS 7750, follow these steps:

-
- Step 1** Click the **Configure** tab on the ICS System Manager home page.
- Step 2** Click **Applications**.
- The page refreshes, displaying a table that contains information about the SPE310s and the applications that are running on them.
- Step 3** Click the desired **CallManager Administration: *IP address*/CCMAdmin** link (where *IP address* is the IP address of the target SPE310 running Cisco CallManager).
- Step 4** Log in to CallManager as an administrator.
-

**Note**

You can also access Cisco CallManager on the Cisco ICS 7750 by entering the following URL, replacing *IP address* with the IP address of an SPE310 running Cisco CallManager: **`http://IP address/CCMAdmin`**.

Accessing SPE310s

You can use Terminal Services Client to access the SPE310 desktop, as described in the following topics:

- [Accessing the SPE310 Windows Interface Through Terminal Services Client, page 5-9](#)
- [Accessing the SPE310 Windows Interface Through Directly Connected Peripherals, page 5-9](#)
- [Accessing SPE310s Through Telnet, page 5-11](#)

- [Accessing the Cisco IOS CLI on ASIs, MRPs, and the SSP Through Telnet, page 5-11](#)
- [Accessing Processor Cards Through the SAP, page 5-12](#)

Accessing the SPE310 Windows Interface Through Terminal Services Client

To access the SPE310 Windows interface through Terminal Services Client, follow these steps:

-
- Step 1** On the PC that you use to administer the Cisco ICS 7750, choose **Start > Programs > Terminal Services Client > Client Connection Manager**.
- Step 2** Use the Client Connection Manager to open a Terminal Services connection with the target SPE310:
- If you already have a Terminal Services Client connection defined for the target SPE310, choose it, and choose **File > Connect**.
 - If you do not have a Terminal Services Client connection defined for the target SPE310, choose **File > New Connection**. Follow the instructions in the wizard. Then choose **File > Connect**.

The Terminal Services Client window opens. You can use Terminal Services Client to access standard Windows utilities on the SPE310, such as Windows Explorer and the Control Panel.

Accessing the SPE310 Windows Interface Through Directly Connected Peripherals

You can connect a monitor, keyboard, and mouse directly to the SPE310 to access the Windows user interface, as follows.



Note

For a summary of the issues related to the connection of peripherals to SPE310s, as well as best practices for using peripherals with SPE310s, see the [“Using Peripherals with SPE310s” section on page 5-19](#).

**Note**

For a list of USB peripherals that have been tested on the Cisco ICS 7750, see the [“Using Peripherals with SPE310s” section on page 5-19](#).

-
- Step 1** Connect the monitor cable to the video port on the SPE310, and power on the monitor.
- Step 2** Do one of the following, based on the type of peripherals that you are using:
- **USB**—Connect a USB keyboard to one SPE310 USB port, and connect a USB mouse to the other SPE310 USB port.
 - **PS/2**—Connect the “Y” splitter cable for your keyboard and mouse to the keyboard/mouse port on the target SPE310. Then connect your keyboard and mouse to the available ends of the “Y” splitter cable.

**Note**

If you are using the “Y” splitter cable to connect a PS/2 mouse and a keyboard to the SPE310, the keyboard and mouse must be connected at or before the time that the SPE310 is rebooted in order to be recognized by the operating system. A USB keyboard and mouse are usually recognized without rebooting the operating system.

-
- Step 3** Use the keyboard, mouse, and monitor to access standard Windows utilities on the SPE310, such as Windows Explorer and the Control Panel.
-

Accessing SPE310s Through Telnet

You can access SPE310s through Telnet, as follows:

-
- Step 1** On a PC, choose **Start > Run**.
- Step 2** Enter the following command to open a Telnet session, where *IP address* is the IP address of the SPE310 that you wish to communicate with:
- ```
telnet IP address 5000
```
- Step 3** Log in as an administrator (user ID *administrator*), and enter your password (the default is *changeme*).
- 

## Accessing the Cisco IOS CLI on ASIs, MRPs, and the SSP Through Telnet

You must use the Cisco IOS CLI to configure the ASIs, MRPs, and SSP. You can open a Telnet or HyperTerminal session to access individual ASIs or MRPs or the SSP so that you can configure them individually, using Cisco IOS software commands.

**Note**

Some Cisco IOS commands are not intended for use on the Cisco ICS 7750 through the CLI. See the [“Best Practices for Using the Cisco IOS CLI”](#) section on page 5-16.

For example, to determine which Cisco IOS software release is running on an ASI, MRP, or the SSP, follow these steps:

- 
- Step 1** Choose **Start > Run**.
- Step 2** Enter the following command to open a Telnet session, where *IP address* is the IP address of the card that you intend to communicate with:
- ```
telnet IP address
```

- Step 3** Enter your login password.
- Step 4** Enter the **show version** command:

```
card> show version
```

Accessing Processor Cards Through the SAP

The SAP provides console access to any other processor card in the Cisco ICS 7750 chassis. By connecting your PC to the console port on the SAP, or by dialing in to a modem that is connected to the console port, you can access a menu that can help you debug and troubleshoot system cards.

To access this text-based menu, follow these steps:

-
- Step 1** If your PC is not already directly connected to the SAP console port, you can use an RJ-45-to-DB-9 adapter with a rolled EIA/TIA-232 cable or the supplied console (blue) cable to make the connection, as follows:

- Connect the SAP console port to an available COM port on your PC.

Or

- Connect a modem to the SAP console port to enable a dial-up connection (9600 baud, maximum).



Note For instructions on how to connect the SAP directly to your PC, refer to the [“Connecting to Card Ports” section on page 3-18](#). For instructions on how connect the SAP a modem and how to configure your modem for remote dial-up access to System Manager, refer to the [“Connecting a Modem” section on page 4-39](#).

- Step 2** On your PC, open HyperTerminal. On PCs running Windows 2000, a typical HyperTerminal path is **Start > Programs > Accessories > Communications > HyperTerminal**.

Step 3 Open a connection with the SAP, as follows:

- If you already have a HyperTerminal connection defined for the SAP, choose **File > Open**, and double-click the appropriate icon.
- If you do not have a HyperTerminal connection defined for the SAP, choose **File > New Connection**, and enter the following information:
 - a. In the Connection Description dialog box, enter a name for the connection in the Name field, select an icon to be associated with the connection, and click **OK**.
 - b. In the Phone Number dialog box, enter the following information:

If the PC is directly connected to the SAP, click the drop-down arrow to view a list of choices for the Connect Using field, choose the PC COM port that is connected to the SAP. Click **OK**.

If the PC is remotely connected (through a modem) to the SAP, click the drop-down arrow to view a list of choices for the Connect Using field, and choose the modem installed in your PC. Then, in the Area Code and Phone Number fields, enter the area code and phone number of the remote Cisco ICS 7750. Click **OK**.
 - c. In the Properties dialog box, click the drop-down arrow to view a list of choices for the Bits per Second field. Choose **9600**, and click **OK**.

A terminal window opens.

Step 4 Press **Ctrl-backslash** (\). A menu similar to the following is displayed:

- A. System Alarm Processor
 - B. MASTER System Processing Engine
 - C. System Switch Processor
-
- 1. Slot 1: Multiservice Route Processor
 - 2. Slot 2: Multiservice Route Processor
 - 3. Slot 3: Multiservice Route Processor
 - 4. Slot 4: Multiservice Route Processor
 - 5. Slot 5: System Processing Engine
 - 6. Slot 6: System Processing Engine

Make a selection to switch:

Step 5 Enter the number or letter that corresponds to the card or slot to which you want to connect.

You are now connected to the selected card, and you can enter the CLI commands that are supported on that card.

Best Practices for Using Microsoft SQL Server

ICS System Manager and Cisco CallManager require Microsoft SQL Server.



Caution

Because of a known issue with Microsoft SQL Server, if you do not install Cisco CallManager on the SPE310 running System Manager, you could expose your network to distributed denial of service (DDoS) attacks. If you do not intend to install Cisco CallManager on the SPE310 running System Manager, you can prevent DDoS attacks by completing the workaround that is provided in the *Release Notes for the Cisco ICS 7750 for System Software Release 2.x.x*.



Caution

Microsoft SQL Server is installed on the SPE310 running System Manager at the factory. If you are reimaging an SPE310 running System Manager, the Image Install Tool installs Microsoft SQL Server. For other SPE310s on which you intend to install Cisco CallManager, Microsoft SQL Server is installed during the Cisco CallManager installation process.

Best Practices for Configuring DHCP

Cisco Network Registrar (CNR) is installed on the SPE310 running System Manager to provide Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) services for the Cisco ICS 7750 and other devices on the LAN to which the Cisco ICS 7750 is connected.

**Caution**

CNR is not intended for use as a standalone software tool on the Cisco ICS 7750. Do not use the CNR CLI or graphical user interface (GUI) to invoke CNR commands on the Cisco ICS 7750.

**Caution**

CNR is factory-installed on the SPE310 running System Manager. Do not attempt to use the CNR installation program to reinstall CNR on the SPE310 running System Manager, and do not attempt to install CNR on any other SPE310s in the chassis. If you are reimaging an SPE310 running System Manager, the Image Install Tool installs CNR automatically.

After the Cisco ICS 7750 has been configured (by running ICSCfg), CNR keeps track of devices that send BOOTP or DHCP requests. A configured SPE310 responds to a DHCP or BOOTP request if the device sending the request has a known MAC address or if the Client Identifier field in the DHCP request is set to a known value.

Installing or Enabling Microsoft DHCP Server on the SPE310 Running System Manager

By default, the Windows image provided with the SPE310 does not have the Microsoft DHCP Server enabled. You should not use the Windows Component Wizard to add or enable the Microsoft DHCP Server on the SPE310 running System Manager. Adding or enabling Microsoft DHCP Server on the SPE310 running System Manager causes a conflict with CNR.

Installing or Enabling a DHCP Server on Other SPE310s or Other Servers

Do not install or enable a DHCP server on the SPE310 that is running System Manager. You can install or configure DHCP on an external server, provided that

- The external DHCP server is configured to *not* respond to DHCP or BOOTP requests from Cisco ICS 7750 cards
- If ICS System Manager is providing DHCP services to IP phones or external DHCP clients, the external DHCP server should not be configured to respond to these hosts
- The DHCP IP address ranges of the external DHCP server must not conflict with the DHCP or BOOTP IP address ranges in use by ICS System Manager

**Note**

If you are using a DHCP server on an external server, consult your DHCP server documentation for additional DHCP configuration guidelines.

SSP Error Messages

If you are using Cisco IOS 12.0(5)WC2b on the SSP, and if you are monitoring the system through a console connection to the SAP, error messages similar to the following might be generated as the SSP boots:

```
% error opening tftp://255.255.255.255/cisconet.cfg (Time out)
% error opening tftp://255.255.255.255/router-config (Time out)
% error opening tftp://255.255.255.255/ciscottr.cfg (Time out)
```

This is an expected condition. The system will continue to operate normally without any external intervention.

Best Practices for Using the Cisco IOS CLI

ICS System Manager is designed to communicate with and to monitor the status of all the components in the chassis. To enable ICS System Manager to perform these functions, a configuration program (ICSCfg) guides you through the configuration process. ICSCfg enables you to change key system parameters, such as the IP addresses of system cards, passwords, destination for syslog messages, and Simple Network Management Protocol (SNMP) community strings.

To enable ICS System Manager to properly function as a system management tool, it is important that you use ICSCfg or ICS System Manager, as appropriate, rather than the Cisco IOS CLI, when you enter key system parameters.

Except for the procedures listed in “[ICSCfg Tasks](#),” you can enter all Cisco IOS CLI commands that are available for use in any Cisco IOS software release that is intended for use on the Cisco ICS 7750.

ICSCfg Tasks

You should always use ICSCfg for the following tasks:

- Passwords
 - Changing the login password, which gives ICS System Manager continued Telnet access to system cards
 - Changing the Windows 2000 administrator password, which grants those with administrator privileges continued access to SPE310s
 - Changing the enable secret or enable password, which makes it possible for administrators to enter certain Cisco IOS commands
- Card configurations
 - Assigning or changing the IP addresses or subnet mask of system cards



Note

When multiple VLANs are configured, the IP addresses and subnet masks of the FastEthernet subinterfaces need to be configured via the CLI.

- SNMP settings
 - Changing read-only and read/write SNMP community strings of the SNMP server
 - Changing the server destination of SNMP traps
 - Managing the SNMP server
- Logging
 - Changing the syslog logging host

**Note**

SNMP community strings and system passwords are case sensitive.

The following tasks should never be configured on the Cisco ICS 7750 by using the Cisco IOS CLI under any circumstances:

- Shutting down an Ethernet interface
- Assigning a system card to a VLAN other than VLAN 1 (the management VLAN)

**Note**

MRP300, MRP3-8FXS, MRP3-16FXS, and MRP3-8FXOM1 cards may be assigned to multiple VLANs. They can be assigned a VLAN other than VLAN 1 as long as they also are members of VLAN 1.

- Disabling Cisco Discovery Protocol (CDP) on an Ethernet or VLAN interface
- Configuring Domain Name System (DNS) on SPEs
- Disabling Network Time Protocol (NTP)
- Invoking the Cisco Network Registrar (CNR) dhcp.exe from c:\program files\network registrar\bin

Saving Configuration Changes

To prevent loss of the ASI or MRP configuration after a reboot, save the running-config file to the startup-config file by following these steps:

	Command	Purpose
Step 1	MRP> enable Password: <i>password</i> MRP#	Enters enable mode. You have entered enable mode when the prompt changes to MRP#.
Step 2	MRP# copy running-config startup-config	Saves the configuration changes to the startup-config file so that they are not lost during resets, power cycles, or power outages.

Using Peripherals with SPE310s

This section summarizes known issues and best practices regarding the use of keyboards, mice, monitors, and the USB CD-ROM drive with SPE310s.

Consider the following issues when using peripherals with SPE310s:

- USB CD-ROM drive:
 - The TEAC 210PU USB CD-ROM drive is included with the Cisco ICS 7750. The TEAC 210PU USB CD-ROM drive is the only USB CD-ROM drive that has been tested for use with SPE310s.
 - Do not connect or disconnect the USB CD-ROM drive while the SPE310 is booting. See the [“Best Practices for Using Peripherals with SPE310s” section on page 5-20](#).
- USB keyboards, mice, and hubs:
 - Because the USB CD-ROM drive is required during reimaging, and because the SPE310 has only two USB ports, a USB hub might be required if you intend to connect both a USB keyboard and a USB mouse to the SPE310, when the keyboard lacks a USB pass-through port.
 - For a list of USB keyboards, mice, and hubs that have been tested with the Cisco ICS 7750, see the [“Connecting a Monitor, Keyboard, and Mouse to the SPE310” section on page 3-26](#).

**Note**

USB devices requiring additional software or installation of non-native Windows 2000 drivers will probably not work with the Cisco ICS 7750. We therefore recommend against trying to use them. If you have additional questions or concerns about using USB devices with the Cisco ICS 7750, contact your Cisco support representative.

- PS/2 keyboards and mice:
 - A “Y” splitter cable is provided with the Cisco ICS 7750 to enable you to connect a PS/2 mouse and a PS/2 keyboard to the SPE310.
 - If you connect a PS/2 device to an SPE310 after the SPE310 boots, the SPE310 will need to be rebooted in order for the PS/2 device to be recognized by Windows 2000.

Best Practices for Using Peripherals with SPE310s

This section describes best practices for using peripherals with SPE310s.

CD-ROM Drive and CD-ROM Drive Tray

The following are best practices for using a CD-ROM drive and the CD-ROM tray with SPE310s:

- Connecting the CD-ROM drive—Do not connect the CD-ROM drive while the SPE310 is booting.
- Disconnecting the CD-ROM drive:
 - If the SPE310 is running, use an attached monitor to locate the Unplug or Eject Hardware icon in the Windows System Tray (in the lower right corner of the screen, typically, unless the taskbar has been moved). The icon looks like a small card with an arrow floating above it. Click the icon. In the pop-up menu displayed, select **Stop USB Mass Storage Device - Drive (D:)**.
 - After Windows 2000 reports that the device has been stopped, you can safely disconnect the USB CD-ROM drive cable from the SPE310 USB port.

**Note**

If you fail to use the Unplug or Eject Hardware tool and if you plug in and unplug the CD-ROM drive many times, the drive may stop responding. If this happens, disconnect the CD-ROM drive, wait 5 minutes, and try reconnecting it again. If the drive still fails to respond, reboot the SPE310; it should be recognized after Windows reboots. If the CD-ROM still fails, contact your Cisco support representative.

- Using the CD-ROM drive tray:
 - A CD-ROM drive tray is provided with the Cisco ICS 7750. The CD-ROM drive tray and the CD-ROM drive are not intended to be connected to the SPE310 for extended periods of time. Leaving the CD-ROM drive tray in place can interfere with airflow into the chassis. Always remove the CD-ROM drive and drive tray when you finish using them.
 - The CD-ROM drive tray is designed only for the weight of the CD-ROM drive. Never place heavy objects or items other than the CD-ROM drive on the drive tray because placing such objects on the tray may damage the ventilation grille or may impede airflow into the chassis.

Keyboards and Mice

The following are best practices for using a PS/2 keyboard and mouse with SPE310s:

- PS/2 keyboards and mice:
 - Connect these devices before booting the SPE310, if possible. If you connect a PS/2 mouse or keyboard to an operational SPE310, you must reboot the SPE310 in order to use the PS/2 mouse or keyboard.
 - Disconnect the “Y” splitter cable from the keyboard/mouse port on the SPE310 when these devices are not being used.

Monitors

The following are best practices for using a monitor with SPE310s:

- Connecting a monitor—Connect the monitor cable to the SPE310 video port before turning on the monitor.
- Disconnecting a monitor—Power down the monitor before disconnecting the monitor cable from the video port on the SPE310.

Determining the IP Address of an SPE310

If you do not know the IP address of an SPE310, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | If your PC is not already directly connected to the SAP console port, use the supplied console cable (blue) to connect the SAP console port to an available COM port on your PC. |
| Step 2 | Open a HyperTerminal session with the SAP (see the “Accessing Processor Cards Through the SAP” section on page 5-12). |
| Step 3 | Log in as an administrator (username <i>administrator</i>), and enter your password (the default is <i>changeme</i>). |
| Step 4 | Press Ctrl-backslash (\), and use the SAP menu to switch to the SPE310 running System Manager (this card is installed in slot 6 by default). |

Step 5 Enter the following command:

```
ipconfig /all
```

Output is displayed that includes information similar to the following:

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . . :  
Description . . . . . : Intel(R) GD82559ER PCI Adapter  
Physical Address. . . . . : 08-00-3E-2D-85-AC  
DHCP Enabled. . . . . : No  
IP Address. . . . . : 10.0.0.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.0.0.1  
DHCP Class ID . . . . . : ICS7750-SPE310
```

Step 6 Record the IP address of the SPE310. You need the IP address of the SPE310 running System Manager to log in to the ICS System Manager interface.

Backing Up System Data

This section explains how to back up SPE310 registry settings, ICS System Manager database records, and Cisco IOS configuration files for ASIs and MRPs:

- [Accessing the Backup Utility, page 5-25](#)
- [Scheduling a Backup, page 5-25](#)
- [Using Backup Now, page 5-27](#)



Caution

Before you back up system data, make sure that no two devices (such as Cisco IP Phones) are assigned the same IP address. If any two devices are using the same IP address, you might experience problems if you later attempt to restore from this backup.

**Note**

The backup procedures in this section do not cover other software that you can install on the system, such as Cisco CallManager. For instructions on how to back up and restore Cisco CallManager data, refer to *Backing Up and Restoring Cisco CallManager 3.3*.

**Note**

Before starting a backup, make sure that at least 75 MB of storage space is available on the target device.

**Note**

Record the SNMP community strings, IP addresses of system cards, and the Windows 2000 administrator password (user ID *administrator*) in a secure location. To restore system data, the system must be configured with the same settings as were in use at the time the backup was made.

**Note**

You cannot currently back up system COM port settings.

**Tip**

Write the IP addresses of system cards on adhesive labels, and affix them to the card faceplates. Record your Windows 2000 administrator password and SNMP community strings in a secure location. Having this information available can facilitate troubleshooting and make it easier to restore system data.

Accessing the Backup Utility

Follow these steps to access the backup utility in ICS System Manager:

-
- Step 1** On a PC, access ICS System Manager (see the [“Accessing ICS System Manager” section on page 5-4](#)).
- Step 2** Click the **System Maintenance** tab.
- The Backup History page appears.
- To schedule a backup, go to the [“Scheduling a Backup” section on page 5-25](#).
 - To immediately start a backup, go to the [“Using Backup Now” section on page 5-27](#).
-

Scheduling a Backup

Follow these steps to schedule a backup.

**Note**

Schedule Backup does not back up all system information. Schedule Backup will back up only SPE310 registry settings, ICS System Manager database records, and Cisco IOS configuration files for MRP and ASI cards that do not have Flash memory (MRP200, ASI160, and ASI81). No configuration files for Flash-based cards will be backed up (MRP300, MRP3-8FXS, MRP3-16FXS, MRP3-8FXOM1, and the SSP). Flash-based cards must be backed up manually.

-
- Step 1** Access the backup utility (see the [“Accessing the Backup Utility” section on page 5-25](#)).
- Step 2** Click **Schedule Backup**.
- Step 3** Enter the required information in the following fields:
- a. Backup Name—A unique name for the backup.
 - b. Description—A statement that can identify the backup.

- c. IP/Hostname—The IP address or host name of the device on which you want to store your backup files.

**Note**

The device on which you intend to store your backup files must be running the Windows operating system.

- d. Shared Pathname—The Windows path name to the remote device (computer on the network) where you want to store your backup files. For example, sharename\path.
- e. User Name—The name that you use to log in to your network.
- f. Password—The password that you use to gain access to your network.
- g. Domain Name—(Optional) The domain name that you use to gain access to your network (for example, MyCompany_Eng).

Step 4 Under Occurrence, click the appropriate radio button:

- Once
- Daily
- Weekly
- Monthly

Step 5 Under Occurrence Date/Time, enter the required information:

- a. Start Date—The date on which this backup should begin.
- b. Time—The time when this backup should begin.
- c. Weekly on—If you selected Weekly at Step 3, the day of the week that the backup should take place.
- d. Monthly on—If you selected Monthly at Step 3, the day of the month that the backup should take place.
- e. End Date/No End Date—Choose the appropriate radio button:
 - End Date—If you do not want this backup schedule to continue past a particular date, click this radio button, and enter the date.
 - No End Date—If you want this backup schedule to continue indefinitely, click this radio button.

Step 6 Click **Submit** to accept the backup parameters that you specified.

Step 7 Click **History**.

The Backup History page displays. The backup schedule that you entered is shown under Existing Schedules.

Using Backup Now

Follow these steps to start the backup process:

Step 1 Access the backup utility (see the [“Accessing the Backup Utility” section on page 5-25](#)).

Step 2 Click **Backup Now**.

Step 3 Enter the required information in the following fields:

- a. Backup Name—A unique name for the backup.
- b. Description—A statement that can identify the backup.
- c. IP/Hostname—The IP address or host name of the device on which you want to store your backup files.



Note

The device on which you intend to store your backup files must be running the Windows operating system.

- d. Shared Pathname—The Windows path name to the remote device (computer on the network) where you want to store your backup files. For example, sharename\path.
- e. User Name—The name that you use to log in to the remote computer.

- f. Password—The password that you use to gain access to the remote computer.
- g. Domain Name—(optional) The domain name that you use to gain access to your network (for example, MyCompany_Eng).

**Note**

Enter the domain name carefully. Because of a limitation in Windows 2000, even if you enter the wrong domain name, the backup will seem to complete successfully.

Step 4 Click **Submit** to start the backup.

Step 5 When the backup is complete, press **Continue**.

The Backup History page appears, showing information about the backup.

Step 6 You must manually back up the Cisco IOS configuration files for the SSP and each Flash-based MRP or ASI card (MRP300, MRP3-8FXS, MRP3-16FXS, or MRP3-8FXOM1).

- a. Telnet to the MRP, ASI, or SSP card from the remote device (computer on the network) where you stored your backup files in Step 3 above.

**Note**

If the remote device (computer on the network) where you stored your backup files does not have Telnet access to the chassis cards, you may save the backup configuration files on a PC that has Telnet access to the chassis cards and then copy them to the remote device.

- b. Enter the **enable** command and your Cisco IOS enable password to enter privileged EXEC command mode:

```
Switch> enable
Password: password
Switch#
```

- c. Enter the following command to display the startup configuration:

```
Switch# show startup-config
```

- d. Copy and paste the output from the show startup-config command into a text file where you stored your backup files:

- Choose **Start > Run**.
- Enter the following command to open Notepad:

notepad.exe

- Select and copy the startup-config output from the Telnet console, and paste it into the Notepad window.

**Note**

Do not include the – More – lines if they are displayed in the output. Select the contents from the Telnet console, and copy them to the clipboard. Go to the Notepad window, and paste the clipboard contents.

If – More– is displayed at the bottom of the Telnet console, press the space bar to display the next screen. Copy from the Telnet console again, and paste to the Notepad window. Repeat until the entire startup configuration has been displayed, copied, and pasted.

- From Notepad, choose File > Save.
- Save the startup-config file under the Shared Pathname you entered in Step 3d in the [“Using Backup Now”](#) section on page 5-27 (for example, \\hostname\sharename\path). Name the config file in this format: <backupname>_<hostname>, where *backupname* comes from the Backup Name in Step 3a in the [“Using Backup Now”](#) section on

page 5-27, and *hostname* is the host name of the card. For example, an SSP configuration file could be named Backup1_Switch, and an MRP300 configuration file could be named Backup1_R00ffff900073.

- Step 7** Repeat Step 6 for the SSP and for every Flash-based MRP or ASI card (MRP300, MRP3-8FXS, MRP3-16FXS, or MRP3-8FXOM1) in the chassis.
- Step 8** If you have configured VLAN functionality on the Cisco ICS 7750, you may also back up the file `vlan.dat` from the SSP Flash memory. This file stores VLAN configuration information.

The procedure for backing up the `vlan.dat` file is the same as the procedure that is used for copying a Flash file to a network server. To copy the `vlan.dat` file to a TFTP network server, use the following command in EXEC mode from the command prompt on the SSP:

```
Switch#copy flash:vlan.dat tftp://<ip address of server>/<dir>/<filename>
```

where *<ip address of server>* is the IP address of the TFTP server, *<dir>* is the directory name on the TFTP server, and *<filename>* is the filename to write on the TFTP server.

Setting Security Privileges

To ensure that only persons with proper authorization have access to sensitive information, you can designate system passwords during initial configuration of ICS System Manager.



Note

For additional information, refer to the ICS System Manager Online Help.

Shutting Down the System

This section describes how to shut down the system.

**Caution**

If your system has only one SPE310, make sure that the system data has been backed up before you remove an operational SPE310. For instructions on backing up system data, see the [“Backing Up System Data” section on page 5-23](#).

Follow these steps to shut down the system:

-
- Step 1** Open a web browser and access ICSConfig:
`http://IP address/icsconfig`
- Step 2** Log in as an administrator (user ID *administrator*), and enter your password (the default is *changeme*).
- Step 3** Click **OK**.
The system discovers the cards that are currently installed in the chassis. After the discovery process is complete, the ICS 7700 System Configuration page displays.
- Step 4** Click **Shutdown/Restart**.
The Restart/Shutdown System Cards page appears.
- Step 5** On the Restart/Shutdown System Cards page, click the **Shutdown** button next to any SPE310 that is not running System Manager.
- Step 6** Click **OK** to confirm that you want to shut down that SPE310.
The STATUS LED on the target SPE310 blinks. When the STATUS LED turns off, the SPE310 is shut down.
- Step 7** Click the **Back** button to return to the Restart/Shutdown System Cards page.
- Step 8** Repeat Step 5 through Step 7 for any additional SPE310s that are not running System Manager.
- Step 9** Repeat Step 5 through Step 7 for the SPE310 running System Manager.
- Step 10** Click the **Back** button to return to the Restart/Shutdown System Cards page.

- Step 11** Click the **Shutdown ICS 7700 System** button.
- Step 12** Press the power switch to off (o) on the power supply modules.
The LEDs on all the other cards will turn off and the fans will stop.
-